Legislative Audit Division

State of Montana

Report to the Legislature

March 2002 **Information System Audit**

Statewide Accounting, Budgeting and Human Resource System (SABHRS) Audit

Department of Administration

This report provides information regarding application controls over the state's central computer system, and general controls over the related processing environment. It contains five recommendations to the department for improving controls over the Statewide Accounting, Budgeting and Human Resource System.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
02DP-02 **Helena MT 59620-1705**

Help eliminate fraud, waste, and abuse in state government. Call the Fraud hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

March 2002

The Legislative Audit Committee
of the Montana State Legislature:

This is the report of our Information System audit of controls relating to the state's central
computer system operated by the Department of Administration. We reviewed specific general
and application controls over the Statewide Accounting, Budgeting and Human Resource System.
This report contains recommendations for improving controls related to the system and
department procedures. Written responses to our audit recommendations are included in the back
of the audit report.

We wish to express our appreciation to the staff of the Department of Administration for their
cooperation and assistance.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Statewide Accounting, Budgeting and Human Resource System (SABHRS) Audit

Appointed and Administrative Officials

Department of Administration	Scott Darkenwald, Director
	Cathy Muri, Administrator Administrative Financial Services Division
	John McEwen, Administrator State Personnel Division
	Brian Wolf, Chief Information Officer Information Technology Services Division
	Tony Herbert, Deputy Chief Information Officer Information Technology Services Division
SABHRS Services Bureau	Chuck Virag, Bureau Chief
	Nyla Johnson Finance Lead
	Jim Sheehy Information Technology Lead
	Theresa Scott Budget Lead
	Martha Watson Human Resource Lead

Introduction

We conduct an annual review of the Statewide Accounting, Budgeting and Human Resource System (SABHRS). SABHRS functions as the state's primary accounting, budgeting, human resource management, and procurement system. We reviewed general controls over the SABHRS processing environment and application controls over Human Resource Management and Finance systems. Background information, audit objectives and audit scope are discussed in chapter I. Audit issues summarized below are discussed in chapters II and III.

General Controls

General Controls are management-developed plans, policies, and procedures applied to the SABHRS environment to assure proper operation of SABHRS computer systems hardware and software. We reviewed the following general control areas: service continuity and security planning, physical and logical access over operating and application software and hardware, software development and change controls, and segregation of duties. Audit issues are summarized below.

▸ Segregation of duties needs to be defined for human resource data access by SABHRS staff.

▸ Service Continuity Plan needs to include operational priorities and needs to be tested for SABHRS application.

▸ Security Plan is necessary that is comprehensive and able to be implemented by SABHRS staff.

Application Controls

Applications are the group of individual computer programs that collectively operate to perform a function. SABHRS applications are Human Resource and Finance. Application Controls are the management-developed plans, policies, and procedures that apply to SABHRS applications and are designed to ensure the application's proper operation.

We reviewed the following application control areas: data acquisition, data processing, and data output. Audit issues are summarized below.

Finance

We reviewed Finance application processing and noted that sufficient information is not retained to enable the review or reconstruction of daily processing. Industry and United States General Accounting Office (GAO) guidance and best practices provide that an audit trail be created to provide evidence of successful processing or to diagnose and manage incident response and restoration. SSB should retain information to support management's ability to monitor processing performance and controls.

▸ Audit trails are necessary to record the history of production and data changes.

▸ Production recovery procedures are necessary for a consistent approach to processing interruptions.

Human Resource

We identified SABHRS Support Bureau staff with unrestricted access to Human Resource production data and observed instances where data was changed without the knowledge or authorization of the data owner to meet production deadlines. Industry and GAO guidance and best practices are that production staff should not have access to production data, and all changes or additions should be tested and approved by the data owner before they are moved into production. SABHRS management and data owners should develop a method that allows SABHRS staff to meet production deadlines and includes data owner authorization of data changes and additions.

Prior Audit Recommendations

The previous audit report contained fourteen recommendations. SABHRS management implemented eight, partially implemented three, and three recommendations were addressed within the scope of the financial-compliance audit of the department.

Conclusion

In conclusion, we identified weaknesses within the SABHRS general controls environment regarding inadequate service continuity and security planning. We also determined the responsibilities and segregation of incompatible duties should be defined.
Overall, the SABHRS applications are processing information as intended; however, we identified areas where the department could

improve by better segregating incompatible duties, planning for security, planning for service interruptions, recording changes to data (audit trail), and developing production recovery procedures when processing stops.

Chapter I - Introduction and Background

Introduction and Background

The Department of Administration (department) is charged with establishing and installing a uniform accounting and reporting system for all state agencies to report the receipt, use, and disposition of all public money and property (section 17-1-102(2), MCA). The Statewide Accounting, Budgeting, and Human Resource System (SABHRS) is the accounting and reporting system used by state agencies for this purpose.

The department is also responsible for operating and maintaining a centralized computer center and associated hardware, software, and services for use by state agencies under terms and conditions established by the department (section 2-17-512 (1)(m), MCA). The department's Information Technology Services Division (ITSD) operates the centralized computer environment. The SABHRS Services Bureau (SSB) exists within ITSD to carry out the responsibility for operating and maintaining SABHRS.

SABHRS Finance and Human Resource Management System Descriptions

SABHRS processing is a combination of commercial software and customized programming. SABHRS components include two applications, the Finance system and the Human Resource Management system.

FINANCE SYSTEM

There are approximately 1,371 Finance system users. The Finance system is composed of five modules:

The **General Ledger (G/L)** module stores balance sheet and revenue and expenditure activity for agencies while separately identifying agency financial activity. Functions include journal entry, budgeting, account inquiry, and reporting.

The **Accounts Receivable (A/R)** module processes and records revenue collections and accounts receivable information. The module has the ability to calculate and store account history, determine receivable aging schedules, create trend analysis, and apply receipts to individual accounts.

The **Accounts Payable (A/P)** module processes and records accounts payable information and manages cash disbursements to vendors. In order to create warrants, agencies must enter payments into the A/P module.

The **Asset Management (AM)** module accounts for state property. The module has the capacity to calculate and record depreciation. Agencies are required to use the module for recording capital assets that exceed $5000 in value.

The **Purchasing (PO)** module automates the goods and services procurement business processes. The department's State Procurement Bureau and Publication & Graphics Bureau are the primary users of the module.

HUMAN RESOURCE MANAGEMENT SYSTEM (HRMS)

There are approximately 3,028 HRMS users. The Human Resource Management System is made up of four modules:

The **Human Resources** module maintains basic information about agency employee positions and compensation plans.

The **Payroll** module provides for online data editing and validation to ensure payroll accuracy, and performs the paycheck calculation process, federal and state tax requirements, direct deposits, garnishments, and savings bonds.

The **Benefits Administration** module automates the process of tracking and distributing benefits, such as sick leave and medical insurance.

The **Time and Labor** module maintains time sheet data, applies all time reporting rules or edits, and provides a direct feed to the Payroll module.

SABHRS application processes and data are the property of individual state agencies. Ultimately, the state agencies remain accountable for agency data, establishing SABHRS reporting objectives and assigning and monitoring agency user security access.

SSB is employed by the agencies to maintain SABHRS systems, manage daily production operations, and operate security.

SSB is comprised of 34 full-time-equivalent positions. SSB charges agencies for the use of SABHRS. SABHRS rates are based on agency number of employees with exceptions for the department's Benefits Bureau and the Montana University System. These exceptions are each assessed a negotiated amount. In fiscal year 2002 and fiscal year 2003, the legislature approved a SABHRS cost allocation to agencies totaling $4,168,460 and $4,211,734, respectively.

Audit Objectives

SABHRS supports the state's core administrative processes of accounting, budgeting, and human resource management. The objective of this audit included identifying and testing selected SABHRS processes and documenting SABHRS and agency responsibilities related to those processes. Our objective is to provide assurances over the following SABHRS general and application controls and processes, and to share our understanding of these processes.

Our general controls audit objectives include evaluating whether SABHRS management performs:

▶ service continuity and security planning based on business needs;

▶ implements and monitors physical and logical access controls over its operating and application systems, and its hardware and software;

▶ has established system development and change control procedures, and

▶ whether the SABHRS environment has adequate segregation of duties.

Our application control objectives include evaluating whether controls exist and operate to ensure agency information processed by SABHRS is reliable.

Audit Scope and Methodology

The audit was conducted in accordance with government auditing standards published by the United States General Accounting Office (GAO). We evaluated controls using generally accepted information technology governance and control practices provided by the GAO.

We requested SABHRS management's description of the SABHRS control environment and evaluated the existence and operation of control activities. Through interview, observation and review of plans, policies and procedures, we evaluated the general controls environment over SABHRS including controls relating to its hardware, software, environmental safeguards, physical and logical access, system development and change controls, continuity planning, and the separation of the incompatible responsibilities of system operations and management of data.

For SABHRS applications, we evaluated whether system access is limited to authorized staff and whether only complete and valid files are accepted for processing. We evaluated whether SSB staff access to data and processing is controlled, whether processing is controlled to allow valid data to process while capturing invalid data, and whether system processing additions or modifications are tested and controlled. We evaluated whether tables and reports are properly updated, whether reports containing processing results and details are available to agency operators and whether reports are reasonably constructed and tested to provide necessary information to agencies.

Prior Audit Recommendations

The previous audit report (00DP-01) contained 14 recommendations. Three recommendations were addressed within the scope of the financial-compliance audit of the department (01-12). SSB implemented eight and partially implemented three

recommendations. The following paragraphs discuss the recommendations that have not been completely implemented.

Recommendations Partially Implemented

Recommendations partially implemented by SSB and discussed in this report include:

▸ We recommended the department define the roles and responsibilities of maintaining SABHRS and segregate system functionality from system data management. (Page 7.)

▸ We recommended SSB update and maintain a formal disaster recovery plan, document procedures for recovering SABHRS applications and test SABHRS recovery. (Page 10.)

▸ We recommended SSB establish security policies and guidelines that define the security responsibilities of the SABHRS and agency operators. (Page 8.)

Introduction

General controls include management developed plans, policies, and procedures intended to create a secure environment over the operation of SABHRS computer system hardware and software. Overall, SABHRS operates in a secure environment, however, we identified opportunities for SSB to improve segregating incompatible duties, planning system security, and planning for unexpected events. These issues are addressed in the following report sections.

Segregation of Duties

The effectiveness of the SABHRS control environment depends on well-defined and properly functioning organizational controls. The organizational structure should ensure the job responsibilities of personnel responsible for maintaining the system are properly separated from the responsibilities of the data owners.

A controlled information systems environment is designed to segregate data ownership and data processing functions. State agencies, as data owners, are responsible for data entry and accuracy including subsequent changes or additions to entered data. SSB is responsible for maintaining the system and managing the data processing programs.

During the prior audit, we determined that SSB personnel took on the responsibilities of identifying and correcting accounting data errors and, therefore, recommended the department define the roles and responsibilities of maintaining SABHRS and segregate system functionality from system data management. SSB now has an agreement with Finance data owners, which defines the circumstances for interventions and authorizes SSB staff to access data. No written agreement exists between SSB and the division authorizing SSB to perform HR data manipulation or delegating agency responsibilities for HR data changes to SSB staff.

During the current audit we observed staff within the SABHRS Support Bureau continuing to perform actions not appropriate for system maintenance staff. We observed SSB staff access HR production data to create unauthorized and undocumented coding

changes to meet processing deadlines. We observed SSB personnel changing HR data to allow continued processing.

The department's State Personnel Division (division) is the process owner for HRMS. Division staff said they were unaware of these processing interventions and neither division staff nor the data owners authorized the additions or changes to the payroll data. Industry standards recommend that segregation exist between system staff responsible for managing the data and system users responsible for data accuracy. Separation of duties is a control meant to ensure no one person has incompatible duties that would permit the perpetration and concealment of errors or irregularities. An organizational structure should include documented definition of data ownership and intervention responsibilities to ensure consistent application of procedures. Defined decisions should include the conditions under which data owners grant access for necessary intervention, and that changes are documented and communicated to the data owner.

Recommendation #1
We recommend the SSB and the State Personnel Division define and formally document the roles and responsibilities of maintaining HRMS data.

Security Plan

Inherent to the operation of automated systems and information use, is the concept of deciding who has access to the system and the information maintained on the system. Industry control objectives state that management is responsible for planning, developing, and implementing a secure control structure over an organization's computer processing environment. These practices usually take the form of a written security plan and are implemented through a security cycle, continually identifying critical functions, assessing risks and monitoring and adjusting security procedures for effectiveness. However, within the SSB environment, there is no complete security plan for how to administer system security and no specific individual designated as the security officer.

SSB has been operating since inception without a complete formal written security plan for the SABHRS environment and SSB staff. We observed SSB staff using pre-SABHRS planning memos and a draft plan dated October 10, 2001, to operate SABHRS security. However, the draft plan and various memos do not address a number of security subjects such as:

‣ The plan does not establish data and processing access for SSB staff based on the principle of "least privilege." Least privilege means only allowing access for the tasks the individual performs.

   We observed various SSB staff with unrestricted access to human resource and finance data. This access allows staff to access raw as well as processed data, to intervene in automated processing procedures, and to access or modify SABHRS processes.

‣ The security plan does not define the SSB security officer who is responsible for granting, implementing, and monitoring SSB access. The security officer should not have data access. We observed SSB staff with data access rights, performing security functions.

‣ SSB staff was not certain how security is structured when questioned about access controls. We attribute this oversight to the lack of a comprehensive security plan.

‣ We noted SSB staff had incorrectly provided an agency employee with unrestricted HR access. We determined the error was caused by lack of clear and concise procedures to guide SSB staff.

‣ Employee position descriptions do not address or establish employee access responsibility, define access level, or monitoring requirements. As a result, SSB staff access is not routinely evaluated or monitored once implemented. We identified a former SSB employee with current access to SABHRS operating system. SSB staff was unsure about revoking access responsibilities.

SSB is the custodian of SABHRS security and therefore is responsible for developing and implementing a security plan. The plan should be a current, comprehensive and organized resource of

security responsibility operation details developed by SSB management and state agencies. The plan is a method of documenting management's security decisions and practices so those participating know their responsibilities and can consistently apply security practices. SSB management should implement the plan and monitor it to ensure consistent and effective security.

Recommendation #2
We recommend the department develop and implement a comprehensive security plan over the SABHRS environment.

Service Continuity

During the previous audit, we recommended the department update and maintain the formal disaster recovery plan, document procedures for recovering SABHRS applications, and test SABHRS recovery. SSB has developed a draft disaster recovery plan dated October 23, 2001, that we reviewed. We acknowledge SSB has made progress towards plan development, and recovery testing was performed. However, we determined the disaster recovery plan needs to include necessary elements such as recovery procedures, incident reporting and follow-up instructions. Input from process owners as to critical functions and sensitive data, and risk assessments for known vulnerabilities are essential yet not provided. Without these considerations, the plan does not identify operational priorities and associated risks.

Since not all SABHRS functions are critical, the plan should be selective and detailed so that risks are addressed, critical functions are prioritized, and resources are applied where needed. The risks the plan is intended to reduce can then be measured against contingency planning costs.

An effective recovery plan should allow management to restore critical computing operations in a reasonable time and to minimize data and production losses. Loss of SABHRS processing functions would impair the majority of state agencies in the ability to process

transactions, provide services to the public, and pay vendors and employees.

> **Recommendation #3**
> **We recommend SSB continue to document and test a comprehensive disaster recovery plan for the SABHRS applications.**

Chapter III – Application Controls

Introduction

An application is a group of computer programs that perform a common function such as creating accounting records. Application controls are the structure, policies, and procedures management develops to ensure applications operate reliably. Overall, SABHRS applications are operating reliably, however, we identified areas where SSB could improve audit trail and production recovery procedures.

SABHRS Audit Trail

An audit trail is an application control that is a transaction's history from when it is input until it is finally recorded on the system. Audit trails are used to backtrack to find the origin of specific information and identify changes that may have occurred to the information.

SABHRS acquires data from state agencies during the business hours of the day and processes the data nightly. If problems occur, SABHRS on-call staff is notified and intervene to continue processing. The on-call staff is composed of ten SSB staff who rotate this responsibility. The on-call staff has access to production data and the ability to redirect the processing workflow as means to continue processing.

We interviewed on-call staff and requested details of the instances when staff had to restart processing. Staff said they do not keep records of all restarts or details and there are no procedures instructing them to do so.

We observed SSB staff upload payroll data from the Human Resource (HR) module to the Finance module. Prior to extracting HR data, staff screen the HR transactions to ensure complete posting to the Finance system. As discussed on Page 7, in the event of errors that would prevent posting, staff directly access the production data and change data to allow payroll to process. SSB staff do not document these changes and additions, leaving no means to reconstruct or identify changes to data. SSB staff said they were not aware of the need for an audit trail and no procedures exist to provide guidance on documenting the changes. Because senior SSB staff do not review the intervention details when staff perform

changes to data or processing, one person is responsible for both authorizing and making the changes.

Industry and GAO guidance and best practices provide that an audit trail should exist to provide evidence of successful processing or to diagnose and manage incident response and restoration. The audit trail should include sufficient information to establish what events occurred and who or what caused them. SSB staff should document data changes in sufficient detail to describe the cause and result of the change. Senior SSB staff should review audit trails of data or processing changes to ensure changes are appropriate.

Recommendation #4
We recommend SSB develop and retain audit trails for data and processing changes.

Production Recovery

Production recovery is a process of restoring or restarting computer application processing after processing has been interrupted and has stopped. SABHRS processing is a sequence of programs and if a program fails, processing halts. In the event of an interruption, SSB staff intervenes to restore processing. We interviewed the staff performing system interventions and determined there is no consistent approach among staff. Staff could not provide similar descriptions of their responsibilities or recovery methods used to restore SABHRS processing. Staff was not able to describe a uniform approach they share for response procedures or identifying critical programs or sensitive data priorities. Staff explained they do what is necessary to ensure payroll and accounting data continue processing. SSB staff said there had been a prior attempt to document SABHRS processing cycle, but the work had not been completed. We attribute the inconsistency to the lack of written procedures to guide them.

Industry and GAO guidance provide that processing interruptions should be included in contingency planning and a methodical approach developed to restore processing. Best practices takes the

form of a written document identifying priority functions to recover, preauthorized levels of data access, incident notification responsibility and tested responses to previously experienced interruptions. Written format is necessary so the information is physically available to assist staff at various locations, can easily be distributed to appropriate personnel, contains information that is a shared understanding for individuals with different experience levels to implement, contains the level of detail necessary for timely and complete response, and staff actions can be consistently applied based on document contents.

The lack of an audit trail, discussed in the previous section, compounds the need for documented procedures to ensure consistent treatment of processing interruptions, enabling management to reconstruct the processing flow if necessary.

Recommendation #5
We recommend SSB develop written SABHRS production recovery procedures.

JUDY MARTZ, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

March 6, 2002

Mr. Scott A. Seacat, Legislative Auditor
Legislative Audit Division
PO Box 201705
State Capitol
Helena, Montana 59620

RECEIVED

MAR 0 6 2002

LEGISLATIVE AUDIT DIV.

Dear Mr. Seacat:

We have reviewed the recommendations pertaining to the Statewide Accounting, Budgeting and Human Resource System (SABHRS) audit conducted for the fiscal year ended June 30, 2001. Our response to the recommendations follows.

Recommendation #1:
We recommend the SSB and the State Personnel Division define and formally document the roles and responsibilities of maintaining HRMS data.

Response:
We concur. SABHRS Services Bureau (SSB) and State Personnel Division staffs are currently collaborating on documents that define the roles and responsibilities each play concerning maintaining HRMS data.

Recommendation #2:
We recommend the department develop and implement a comprehensive security plan over the SABHRS environment.

Response:
We concur. We have devoted a great deal of attention to establishing an appropriately secured environment for our SABHRS operators and providing guidance to agency security officers. Our attention is now focused on developing a comprehensive security plan that includes a component addressing the SABHRS support environment. The Information Technology Services Division's Information Security Service Delivery Team will assist this effort. The purpose of this Team is to review security policy and make related recommendations for enterprise applications like SABHRS.

Recommendation #3:
We recommend SSB continue to document and test a comprehensive disaster recovery plan for the SABHRS applications.

Response:
We concur. Disaster recovery and business continuation planning is a high priority for the Department and the Information Technology Services Division. The Division has formed two service delivery teams tasked with developing statewide guidelines for disaster recovery and business continuation planning, and establishing related plans for applications supported by the Division, including the SABHRS. In addition, we will continue to test recovery procedures for the SABHRS applications. To-date, we have successfully restored the budget and human resource applications during disaster recovery testing at our remote site.

Recommendation #4:
We recommend SSB develop and retain audit trails for data and processing changes.

Response:
We concur. SSB management is currently writing procedures that provide guidance regarding the appropriate response to system problems occurring during nightly batch processing, and the related audit trail documentation and review requirements. We are also evaluating whether system related tools could assist with documenting the process flow. In addition, in conjunction with the effort described in our response to recommendation #1, SABHRS Services Bureau and State Personnel Division staffs are developing written guidelines describing the conditions under which SSB staff may change data, and the related audit trail documentation and review requirements.

Recommendation #5:
We recommend SSB develop written SABHRS production recovery procedures.

Response:
We concur. As noted in our response to recommendation #4, SSB management is currently developing written procedures that will provide guidance to staff regarding the appropriate response to system processing problems.

We recognize the significance of the recommendations contained in the audit report and will make compliance a high priority. We thank you and your staff for conducting the SABHRS audit in a professional manner.

Sincerely,

Scott Darkenwald

SCOTT DARKENWALD
Director